07/13/04 - COMMISSION ADVISORY LETTER 2004-1

COMMISSION ADVISORY LETTER 2004-1

SUBJECT: Electronic Voting Security

Under the Help America Vote Act of 2002 (HAVA), the United States Election Assistance Commission (EAC) is charged with "serv[ing] as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of federal elections. . . ." 42 U.S.C. § 15322. While the EAC cannot issue a formal advisory opinion, the EAC concludes that it is appropriate and consistent with its duties under the HAVA to occasionally offer its general views on important issues and questions that arise under HAVA. The opinions expressed in this letter are not binding on the EAC, its staff, or on any person with rights, duties, or obligations under HAVA.

On May 5, 2004, in Washington, D.C., the EAC conducted a public hearing on the usability, reliability, and security of electronic voting systems. The evidence and testimony received at this hearing indicates that the use of electronic voting systems (e.g., "touchscreen voting") is rapidly emerging as an important technological trend in the administration of elections nationwide. Many Americans will vote on electronic or computer-based voting systems in the November 2004 federal election, including disabled voters and voters who speak a language other than English, for whom these systems have important advantages.

At the May 5th hearing, the EAC also received evidence and testimony about the security of electronic voting systems. The EAC is aware of an ongoing national debate, among academics, election administrators, and advocates on this issue of the security of electronic voting systems.

In light of these circumstances, the EAC finds that it is appropriate to provide advice on security needs related to the use of electronic voting devices. Specifically, the EAC advises the following steps to insure election integrity and promote voter confidence:

1. Every election jurisdiction that uses electronic voting devices should identify and implement enhanced security measures in November. EAC will create a Tool Kit that offers guidance on specific methods and will assist in the identification and execution of security methods when needed.
2. All voting software vendors should allow election officials with whom they have contracted to analyze the proprietary source code of their software and to protect that process by using appropriate nondisclosure and confidentiality agreements. EAC will assist in the analysis when needed.
3. Every voting software vendor should submit their certified software to the National Software Reference Library (NSRL) at the National Institute of Standards and Technology (NIST). This will facilitate the tracking of software version usage. NSRL is designed to collect software from various sources and incorporate file profiles computed

from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. The NSRL was built to meet the needs of the law enforcement community for rigorously verified data that can meet the exacting requirement of the criminal justice system.

4. The EAC will solicit information about suspicious electronic voting system activity including software programming and will request aggressive investigative and prosecutorial responses from the U. S. Department of Justice Elections Crimes Branch in the Criminal Division.

5. EAC will document incidents and record data concerning electronic voting equipment malfunctions in November. This information will be submitted to the EAC Technical Guidelines Development Committee that will be creating the new voluntary voting systems standards.

_____

DeForest B. Soaries, Jr.

Chairman

U.S. Election Assistance Commission